TASK ORDER(TO)

47QFCA19F0006

Information Technology Enterprise Management Systems Solution (ITEMSS)

in support of:

Product Lead (PL) Reserve Component Automation System - Force Management System (RCAS - FMS)

Issued to:
CACI, Inc.
(GSA) Alliant 2 Unrestricted Governmentwide Acquisition Contract (GWAC), Multiple Award, Indefinite Quantity (IDIQ) Contract

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

April 25, 2019

FEDSIM Project Number AR00980

C.1 BACKGROUND

C.1.1 PURPOSE

The purpose of this effort is to provide performance-based Information Technology (IT) enterprise management systems solutions services in support of Product Lead (PL) Reserve Component Automation System - Force Management System (RCAS - FMS). These encompass services associated with the Reserve Component Automation System (RCAS), Force Management System (FMS), Defense Readiness Reporting System – Army (DRRS-A), National Guard Bureau (NGB) Information Management Architecture (IMA) Division, Army National Guard (ARNG) Distance Learning Program (DLP), and associated projects, programs, applications, and infrastructure services in support of the Product Lead (PL) and its clients. This support to PL RCAS-FMS includes a broad range of supporting and IT engineering services in domains that include design, software, hardware, network, cybersecurity, and Military Construction (MILCON) IT tails (IT build-out) services.

C.1.1.1 VISION

The PL RCAS-FMS vision is two-part. First, PL RCAS-FMS will deliver a Total Army Force Management capability that meets automation requirements across the entire spectrum of the Army Force Management Model based on the consolidation and enhancement of RCAS, FMS, and DRRS-A into a single solution. Second, PL RCAS-FMS will continue to meet the unique automation and hardware infrastructure needs for the Army Reserve Component (RC), which consists of the ARNG and United States (U.S.) Army Reserve (USAR), by supporting the NGB IMA Division, DLP, and IT build-out efforts.

In pursuit of this vision, PL RCAS-FMS values a collaborative relationship with Industry that incrementally, rapidly, and efficiently delivers working software and infrastructure solutions to the field; reinvests resources into people, processes, and technology; and establishes a highly adaptive culture that drives change and innovation.

There are four major focus areas that realize this vision:

a. Satisfy Stakeholder Needs.
b. Sustain Legacy Systems and Infrastructure while Modernizing the Enterprise.
c. Maintain Audit and Regulatory Compliance.
d. Implement Agile with an Integrated DevSecOps Pipeline.

Currently (“as-is”), PL RCAS-FMS is the acquisition lead for programs and products under RCAS, FMS, and DRRS-A, supports the NGB IMA Division’s mission, and executes a series of IT infrastructure (e.g., design, engineering, and integration) efforts in support of both the ARNG and USAR. RCAS, FMS, and DRRS-A were previously managed independently from each other (see **Section J, Attachment F**, Current IT and Network Environment)**.**

At present (“transitory”), PL RCAS-FMS is combining RCAS and FMS into a single acquisition oversight program and implementing the Global Force Management Data Initiative (GFM DI) data standard for the Army, while sustaining legacy systems, infrastructure, and processes. PL

RCAS-FMS is actively supporting the Enterprise concept by transitioning RCAS personnel management capabilities into the Integrated Pay and Personnel System – Army (IPPS-A), planning for the transition of other RCAS Safety capabilities into the Army Safety and Occupational Health Management System (ASOHEIMS), identifying capabilities across all program areas to be decommissioned, and designing and developing a Total Army Force Management capability in collaboration with the Headquarters (HQ) Department of the Army (DA) G-3/5/7 Global Force Information Management (GFIM) Capability Management Office (CMO). PL RCAS-FMS will begin the development of a Total Army Force Management capability with the consolidation and enhancement of RCAS, FMS, and DRRS-A into a single system. In parallel, the ARNG IMA Division is managing the migration of their IT capability such as SIDPERS into IPPS-A Increment II. PL RCAS-FMS is also planning to transition portions of DRRS-A to the Office of the Secretary of Defense (OSD).

In the future ("to-be"), PL RCAS-FMS envisions that it will combine RCAS and FMS into a unified acquisition program based on the implementation of GFM DI through the enhancement of the FMS Program's Army Organization Server (AOS) and AOS Data Interface (AOS DI). The AOS and AOS DI provide the technical framework that makes it possible to modernize and consolidate the entire FMS portfolio and components of RCAS and DRRS-A into a Total Army Force Management capability for all Army Components across multiple functional domain areas. As PL RCAS-FMS modernizes and consolidates legacy capability that is currently provided by RCAS, FMS, and DRRS-A, the HQ DA G-3/5/7 GFIM CMO envisions that PL RCAS-FMS will develop the programmatic and technical basis to consolidate additional systems and capability within the GFIM CMO's portfolio of systems. In addition, PL RCAS-FMS will complete the transition of applicable RCAS capability into IPPS-A and ASOHEIMS and transition some DRRS-A capabilities to OSD while responsibly managing the decommissioning of irrelevant or duplicative systems. Further, NGB IMA Division will complete their portion of capability migration to IPPS-A while sustaining remaining IT capability for the ARNG. PL RCAS-FMS anticipates that the conditions and timelines for transitioning capability to external efforts such as IPPS-A, ASOHEIMS, and OSD may change given a variety of dependencies and the plan and execution of the future state will allow for flexibility in implementing these transitions. However, until the full and complete transition, PL RCAS-FMS will fully support these programs to prevent a gap in support to the soldier. PL RCAS-FMS will continue to support the acquisition and contracting needs in support of the NGB IMA Division, deliver ARNG DLP and IT infrastructure and IT build-out solutions for the ARNG and USAR, and maintain a leading position in the Department of Defense (DoD) as an innovator to deliver solutions to the soldier.

C.1.2 AGENCY MISSION

C.1.2.1 RCAS-FMS PRODUCT OFFICE (PO)

The Program Executive Office Enterprise Information Systems (PEO EIS) mission is to rapidly deliver innovative and cost-effective systems and services for the Total Force, to globally connect the Army and provide a decisive information advantage to every soldier. PEO EIS develops, acquires, and deploys tactical and management IT systems and products. Within PEO EIS, the RCAS-FMS PO is organizationally aligned under Program Manager (PM) IPPS-A, the responsible O-6 Command. The RCAS-FMS PO is responsible for the total life cycle management of multiple software applications directly enabling the Army's mobilization, training, force development, documentation, and management missions. In 2017, PEO EIS

consolidated the acquisition oversight for RCAS, FMS, and DRRS-A into a single PO called RCAS-FMS.

PL RCAS-FMS is responsible for the following programs and projects: RCAS (sustainment of applications and network hardware for ARNG and USAR); support of ARNG IMA applications; design and implementation of IT solutions for ARNG and USAR; and ARNG DLP, FMS, and DRRS-A. These programs and projects are further defined below.

C.1.2.2 RCAS

The RCAS Program is a Congressionally-mandated program that enables both the ARNG and USAR to maintain readiness with IT service and IT hardware procurements. RCAS IT service procurements support business application management, software, database, and web development and application support to enable the ARNG and USAR with standardized and sustainable Automated Information Systems (AIS). The RCAS Product consists of an integrated web, database, and infrastructure solution that serves functional requirements in the Force Authorization (FA), Personnel (PER), Safety (SOH), and Mobilization (MOB) domains. PL RCAS-FMS is responsible for sustaining and deploying the RCAS Product to serve the ARNG and USAR across all 50 States, three Territories, and the District of Columbia (D.C.). RCAS IT hardware procurements support additional IT hardware and network integration and modernization efforts for ARNG and USAR.

C.1.2.3 FMS

The FMS Program is a Family of Systems (FoS) and Authoritative Data Sources (ADS) that enable the Army to execute force development, documentation, and management operations. The FMS FoS consists of the Structure and Manpower Allocation System (SAMAS), FMS Modified Table of Organization and Equipment (FMS MTOE), FMS Table of Distribution and Allowances (FMS TDA), AOS, AOS DI, and AOS Decisive Action Training Environment (AOS DATE). Functionally, the FMS FoS also satisfies functional needs for Basis of Issue Plan (BOIP) and Tables of Organization and Equipment (TOE). Force management is the overall framework on which the Army is raised, maintained, and sustained. Force development, a sub-process of force management, determines organizational and materiel requirements and translates them into time-phased programs and force structure to accomplish Army missions and functions. Unlike RCAS, FMS is primarily focused on acquiring IT services, such as software development and related engineering efforts, to deliver web-enabled capability to the Army. FMS is the leading program for implementing GFM DI for the Army.

C.1.2.4 DRRS-A

The DRRS-A Program is the Army's ADS for Unit Identification Codes (UIC) and executes three key missions: force registration, force readiness, and force projection. These missions allow the Army to mobilize and demobilize units, report to other DoD and Joint systems and organizations, and enable other ADSs that service logistics and human resource operations. Similar to FMS, DRRS-A is primarily focused on acquiring software development and integrated infrastructure and engineering efforts to deliver web-enabled capability to the Army. PL RCAS-FMS anticipates transitioning some DRRS-A capabilities to OSD while others will remain as part of this TO.

C.1.2.5 ARNG DLP

The DLP is a congressionally mandated program designed to improve military readiness, enhance Command, Control, Communications, and Computers (C4), and practically serve America's communities by making available shared access to high-performance communications. DLP provides digital distance-learning-oriented classrooms to train soldiers, thereby, increasing National Guard (NG) readiness, promotes shared use to make classrooms available for use by the civilian community, and allows Warfighters and their families to communicate between home station and deployed unit locations. PL RCAS-FMS supports ARNG DLP by providing the ARNG the means to procure hardware and associated labor to deliver IT capability required to operate DLP classrooms.

C.1.2.6 ARNG IMA DIVISION

The ARNG is an operational organization providing trained and deployment-ready soldiers from the 50 States, U.S. Territories, and D.C. The ARNG is fully capable of accomplishing state, national, and international missions during war and peace. To meet these requirements, the ARNG maintains a balanced mix of combat, combat support, and combat service support units. These units are structured to integrate seamlessly within AC units, as needed, and are located in nearly 3,000 communities throughout the U.S., which enables them to respond rapidly to domestic emergencies. Similar to RCAS and FMS, IMA Division is managing the transition of its personnel systems to IPPS-A throughout multiple Increments and Releases. The following systems operate under the purview of ARNG IMA Division:

a. AFCOS/JUSTIS: Automated Fund Control Orders System / JUMPS Standard Terminal Input System
b. EDW: Enterprise Data Warehouse
c. eFLIPL: Electronic Financial Liability Investigation of Property Loss
d. GIS: Geospatial Information System
e. MUP: My Unit Pay
f. SIDPERS: Standard Installation/Division Personnel System
g. TAPDB-G: Total Army Personnel Database-Guard

The IMA Division is part of the ARNG G6 organization of the ARNG HQs. The ARNG IMA Division is responsible for providing a broad range of IT services to the ARNG. The IMA Division includes branches responsible for Application Sustainment and Development, Data Center Operations, and Data Management.

C.1.2.7 IT INFRASTRUCTURE INTEGRATION AND REFRESH (ITII&R)

The USAR G6 is currently responsible for the IT requirements of IT build-out work projects for new and existing Army Reserve and United States Army Civil Affairs and Psychological Operations Command (USACAPOC) facilities throughout the U.S.

C.2 SCOPE

The scope of this effort is to sustain, enhance, modernize, consolidate, and decommission software and infrastructure capability in support of PL RCAS-FMS, including a broad range of IT engineering services in design, software, hardware, network, cybersecurity, and IT build-outs.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

Detailed information on the current IT and network environments supported can be found in **Section J, Attachment F**, Current IT and Network Environment.

C.3.1 FUTURE ENVIRONMENT

As indicated in **Section C.1.1.1**, the U.S. Army continues its drive to the enterprise model, and in doing so will support the enhancement and integration of current RCAS, FMS, and DRRS-A systems to be integrated into Total Army Force Management, IPPS-A, ASOHEIMS, and OSD, as applicable to each program area.

The future IT architecture shall be sufficiently sized, maintained, and robust enough to support the timely execution of workload. The implemented hardware, software, and network upgrades, shall ensure integration and compatibility with the most current Army architectural directives.

The enhancement of the FMS Product shall support consolidation into the Total Army Force Management solution pursuant to the PL RCAS-FMS vision and mission.

C.4 OBJECTIVE

The objectives of this effort are to:

a. Rapidly and incrementally deliver quality, working software in an innovative, timely, and cost-effective manner to the soldier.

b. Establish a singular and unified enterprise management systems solutions services.

c. Execute the complete transition of systems to the appropriate Enterprise solution for other applications under PL RCAS-FMS, execute application rationalization and subsequent decommissioning as directed. Sustain all applications until subsumed or decommissioned.

d. Maintain the underlying infrastructure that supports PL RCAS-FMS systems and consolidate and enhance that infrastructure in sync with application enhancement and consolidation pursuant to DoD initiatives for Cloud migration and consolidation; and establishment of an enterprise hosting solution for all PL RCAS-FMS systems

e. Sustain and execute delivery of IT capability (solutions for automation, software, hardware, and networking) to support the ARNG and USAR in the IMA, DLP, and IT build-out for ITII&R areas.

f. Sustain, enhance, consolidate, and decommission NGB IMA Division applications and infrastructure as a nested part of the Army and ARNG's overall effort to deploy enterprise capabilities in secure common operating environments.

C.5 TASKS

The major task areas of the Information Technology Enterprise Management Systems Solution (ITEMSS) TO are defined below:

a. Task 1 – Provide Program Management
b. Task 2 – Software Engineering
c. Task 3 – IT Infrastructure and Network Engineering

d. Task 4 – Cybersecurity
e. Task 5 – Enterprise Help Desk Support
f. Task 6 – Training
g. Task 7 – Innovation
h. Task 8 – Surge/Special Projects Support (Optional)

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management including management and oversight of all activities performed by contractor personnel and subcontractors.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the PL RCAS-FMS via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported NLT October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROGRAM KICK-OFF MEETING

The contractor shall schedule and coordinate a Program Kick-Off Meeting (**Section F, Deliverable 2**) at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from the directorates, other vital Government personnel, and the FEDSIM COR. At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 1**) for review and approval by the FEDSIM COR and the RCAS-FMS PO Technical Point of Contact (TPOC) prior to finalizing. At minimum, the contractor shall include the following topics/deliverables in the agenda:

a. Points of Contact (POCs) for all parties.
b. Transition Discussion.

The contractor shall provide the following at the Kick-Off Meeting:

a. Draft Program Management Plan (PMP) (**Section F, Deliverable 16**).

b. Software Development Plan (SDP) (**Section F, Deliverable 4**).
c. Earned Value Management (EVM) Plan (**Section F, Deliverable 5**).
d. Enterprise Quality Assurance Plan (EQAP) (**Section F, Deliverable 6**).
e. Risk Management Plan (RMP) (**Section F, Deliverable 7**).
f. Cybersecurity Management Plan (CsMP) (**Section F, Deliverable 8**).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

C.5.1.3 SUBTASK 3 – EXECUTIVE-LEVEL PROJECT STATUS BRIEFINGS

The contractor shall develop Executive-level Project Status Briefings (**Section F, Deliverable 9**). The contractor shall develop presentations to include a visual presentation with handouts for each attendee.

C.5.1.4 SUBTASK 4 – ENTERPRISE COORDINATION MEETINGS

The contractor shall coordinate and conduct Enterprise Coordination Meetings (**Section F, Deliverable 10**).

At a minimum, the enterprise coordination meetings will be held on the following topics:

a. Cybersecurity
b. Enterprise Engineering
c. Configuration Management (CM)
d. Quality Assurance (QA)
e. Risk Management
f. Product Area Discussions

The contractor shall develop and deliver Enterprise Coordination Meeting Agendas (**Section F, Deliverable 11**) for each requested Enterprise Coordination Meeting and deliver the agenda to the FEDSIM COR and RCAS-FMS TPOC.

The contractor shall prepare and deliver meeting minutes (**Section F, Deliverable 12**) to the FEDSIM COR and the RCAS-FMS TPOC.

C.5.1.5 SUBTASK 5 – STATUS REPORTS

The contractor shall host a meeting to provide a status update, as required by the Government (i.e., the summary of that week's particular activities that pertain to each task). Status Reports (**Section F, Deliverable 13**) will be used as spot checks to ensure continuous monitoring of the project's progress. The following information may be addressed in each report:

a. Progress as per schedule and milestones.
b. Progress on assigned tasks in support of software development and maintenance.
c. Progress in the development of requirements.
d. Progress on software/hardware purchases.
e. Obsolescence.
f. Cybersecurity.

C.5.1.6 SUBTASK 6 – PREPARE INTEGRATED PROGRAM MONTHLY REVIEW (IPMR)

The contractor shall develop an IPMR (**Section F, Deliverable 14**) using Microsoft (MS) Office Suite applications and deliver it via electronic mail (email) to the RCAS-FMS TPOC and the FEDSIM COR. The contractor shall include the following items in the IPMR:

a. Activities during the reporting period, by task (including ongoing activities, new activities, completed activities, and progress to date on all above mentioned activities). Each section will begin with a brief description of the task.
b. Risk and issue tracking including, strategies, and corrective actions.
c. A Staffing Plan that includes initial filling of billets as well as ongoing contingencies to handle personnel turnover and areas of shortfall.
d. Program Schedule (including major tasks, milestones, and deliverables as well as planned and actual start and completion dates for each milestone).
e. Summary of trips taken.
f. EVM statistics as per **Section C.5.1.8**.
g. Costs for each CLIN for the current month and TO year to date.
h. Projected cost of each CLIN for the upcoming month.
i. Cost and schedule comparison data/monthly performance reports.
j. Metrics on problem areas such as trouble tickets, help desk tickets, and System Problem Reports (SPRs), whether identified by the Government or the contractor. Metrics on problem areas shall include a trend analysis.
k. Integrated Baseline Review (IBR) (**Section F, Deliverable 15**).

C.5.1.7 SUBTASK 7 – PREPARE AND UPDATE A PMP

The contractor shall develop and deliver a Draft (**Section F, Deliverable 16**) and Final PMP (**Section F, Deliverable 17**) that is based on the contractor's proposed solution. Upon Government approval, the contractor shall execute the PMP. The PMP is an evolutionary document, and as such, the contractor shall provide PMP updates throughout the TO performance period as changes in management items occur. The contractor shall update all appropriate sections of the PMP that are affected by these changes.

The contractor shall operate under a Government-approved PMP at all times. The contractor shall include the following items in the PMP:

a. All support requirements in the PMP.
b. A description of the contractor's organization, resources, processes, and management controls that will be employed.
c. A staffing plan.
d. The proposed organizational structure (including responsibilities and reporting structure), how personnel will be assigned throughout the contractual period, and how the proposed project team will interface with both the contractor's corporate structure and the Government command structure.

e. The contractor's management process, subcontractor management process, external contractor communication plan (for integrating IT tasks outside the scope of this TO), and communication plan with the Government.
f. The contractor's Standard Operating Procedures (SOPs) for all operational and developmental tasks (e.g., general operating procedures for travel, leave, work hours, problem resolution, the technical direction plan process)
g. Define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification of risks and resolution of issues
h. The Integrated Master Schedule (IMS).
i. A Work Breakdown Structure (WBS), and associated responsibilities and partnerships between Government organizations by which the contractor shall manage all work.
j. The contractor's SDP and EVM Plan.

C.5.1.8 SUBTASK 8 – EVM CRITERIA

The contractor shall employ and report on EVM in the management of this PWS (see **Section H.13**). While the Government reserves the right of final approval, a joint determination will be made by the Government and contractor as to where EVM will be applicable. Specific task areas requiring EVM will be further defined IAW **Section H.19**.

C.5.1.9 SUBTASK 9 – PREPARE AFTER ACTION REPORTS (AAR)

The contractor shall retain a summary of all long-distance travel, to include, at a minimum, a detailed description of the purpose of the trip, and any knowledge gained (**Section F, Deliverable 18**). The Government will identify the need for an AAR when a request for travel is submitted or after participating in a meeting, discussion, conference, seminar, training, event, etc.

C.5.1.10 SUBTASK 10 – ASSET MANAGEMENT

The contractor shall institute property control and accountability procedures to safeguard and maintain all Government Furnished Property (GFP), including Contractor Acquired Property (CAP), in accordance with **Section H.2** – Government Furnished Property. The contractor shall submit a Government Property Report (**Section F, Deliverable 19**).

The contractor shall assist PL RCAS-FMS in entering data into its designated Defense Property Accounting System.

C.5.1.11 SUBTASK 11 – ENTERPRISE RISK MANAGEMENT

The contractor shall establish and maintain an enterprise Risk Management Program that identifies and mitigates risks across the entire portfolio (i.e., programmatic and technical risks in areas such as cost and schedule). In support of Enterprise Risk Management, the contractor shall develop a Risk Management Program to formalize how risk management activities will be conducted. The contractor shall leverage automation to identify, report, and mitigate risk with transparency and efficiency and support the Government to comply with applicable audit and DoD regulations and policies regarding risk management. The contractor shall leverage the RMP to identify opportunities for innovation and to also inform the development of the RCAS-FMS technology roadmap.

The contractor shall update the RMP on a monthly basis, or when changes impact the execution of the requirements, to enable PL RCAS-FMS to make timely and informed decisions and allocate resources appropriately. The contractor shall provide the following components in the RMP:

a. An outline of the methodology that the program will use to continuously identify, analyze, measure, and mitigate risks.
b. Definitions, assumptions, risk breakdown structure, risk register, and matrices for likelihood/consequence and confidence.
c. Plan of Action and Milestones (POA&M) to mitigate risks.

Along with the RMP, risk identification, mitigation, and reporting shall be provided in a Risk Identification Worksheet (**Section F, Deliverable 20**). In the Risk Identification Worksheet, The contractor shall provide and submit to the Government, at minimum, the key risks that need to be elevated to the Government for cost, schedule, and performance.

C.5.1.12 SUBTASK 12 – ENTERPRISE CM

The contractor shall establish an enterprise CM Program, develop a Configuration Management Plan (CMP) (**Section F, Deliverable 21**), and establish and maintain a strict change control process. The change control process shall include hardware, applications, database, and updates for all PL RCAS-FMS supported programs and projects. Through the CM program, the contractor shall provide support for the Government to monitor and track the configuration of all aspects of the program at any time.

The contractor shall coordinate with the FEDSIM COR and PL RCAS-FMS TPOC on changes to the environment through the change control process outlined in the contractor CMP and IAW the Government's CM guidance.

The contractor shall provide an innovative approach to maintain CM requirements for software, hardware baselines, and Engineering Change Proposals (ECPs) in response to security vulnerabilities, directed architecture changes, policy/regulatory changes, legislative changes, interface changes, Business Process Improvements (BPIs), and environmental changes.

The contractor shall manage strict version control on all software source code and related artifacts either acquired or developed per the Government-accepted CMP. The contractor shall:

a. Maintain the baselines and documentation for all system releases.
b. Monitor and report the installation status of each new release.
c. Provide a CM tool based on industry best practices. The tool shall provide the Government with access to the latest CM documentation.
d. Apply CM through the entire lifecycle of all technology including:
    1. Preparation of CM documentation for enterprise and project artifacts.
    2. Participation in CM planning.
    3. Oversight and participation in library setup and control for all developmental components and products; participation in the identification and marking of baseline product components.
    4. Participation in process improvement initiatives.
    5. Supporting technical configuration control boards.

6. Developing, documenting, and executing CM policies, processes, and SOPs.
7. Establishing proper control and coordination of all documents generated such that all data deliverables are on time and fulfill routine requests for published documents.

The contractor shall maintain the baselines and documentation for all system releases and provide an enterprise release strategy (**Section F, Deliverable 22**). The contractor shall monitor and report the installation status of each new release. This shall include source code control, baseline management, and documentation control.

C.5.1.13 SUBTASK 13 – ENTERPRISE QUALITY ASSURANCE (EQA)

Effective EQA management shall have sufficient, well-defined responsibility, authority, and the organizational freedom to identify and evaluate quality problems and initiate, recommend, and/or provide solutions.

The contractor shall plan, develop, document, and implement an EQA Program that addresses both hardware and software to be defined in the EQAP (**Section F, Deliverable6**) to ensure that comprehensive quality is attained. Within the EQAP, the contractor shall identify its approach for providing quality assurance in meeting the PWS requirements. The contractor shall describe its quality assurance methodology for accomplishing PWS performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The contractor shall describe how the processes integrate with the Government's requirements.

The contractor shall provide enterprise quality assurance across products' lifecycle including unit, integration, regression, and security (e.g., Security Technical Implementation Guide (STIG)) testing to ensure the delivery of quality DoD-compliant products. The contractor shall provide a final baseline EQAP as required in Section F. The contractor shall periodically update the EQAP, as required in Section F (**Section F, Deliverable 23**), as changes in program processes are identified.

The contractor shall maintain an EQA Program that adheres to industry standard. The term EQA Program Requirements, used herein, includes the collective requirements of the standard. The contractor's EQA Program shall adhere to industry-recognized standards. The contractor's EQA Program shall be applied to IT requirements; IT design; IT engineering standards, practices, and procedures; computer program implementation; software documentation; software and hardware testing; software library controls; CM; corrective action; and subcontractor administration.

The contractor shall deliver objective evaluations and quality reports on software (**Section F, Deliverable 24**). Results of all EQA activities shall be documented in industry best practice formats and shall be delivered to the FEDSIM COR and PL RCAS-FMS TPOC.

The contractor shall provide DoD-compliant QC t across product lifecycles that is fully integrated with the enterprise production environment and tested to include hardware, software, security, operating systems, Operating Systems (O/S), and networks. The contractor shall develop and implement procedures to identify, prevent, and eliminate non-recurrence of defective services.

The contractor shall provide enterprise activities of QA and metrics, risk management and lessons learned programs/data repositories, programmatic CM, programmatic asset management,

facilities management, lab management, test and evaluation management, enterprise customer relationship management, liaison activities, and portal management.

C.5.1.14 SUBTASK 14 – INTEGRATED DATA ENVIRONMENT (IDE)

The contractor shall develop and maintain a secure, Common Access Card (CAC)-enabled IDE that includes a real-time, seamless, and collaborative environment for the contractor and the Government. The IDE shall enable access to the contractor's software development environment, providing authorized Government stakeholders with on-demand, on-line access to work products under development commencing at the start of work.

The contractor's IDE shall host all data referenced or produced, including cost, schedule, and technical data and deliverables. This data management program, including IDE structure, format, processes, and procedures shall be documented within the PMP.

The IDE shall contain, at a minimum, the following information:

a. Approved and pending deliverables and associated workflow/status (e.g., pending delivery, delivered pending Government acceptance, or Government accepted).
b. Knowledge management (e.g., CLIN cost data, audit information, and historical artifacts).
c. Inventory management (e.g., hardware and software licensing).
d. Workflow (e.g., accounting, invoicing, approval estimates, travel, and Requests to Initiate Purchase (RIPs)).
e. Integration with program environment (e.g., software environment, help desk, and enterprise services).

The contractor shall inform the FEDSIM COR and RCAS-FMS TPOC of any additional data items not specified in Section F, Deliverables, in support of the processes/procedures that the contractor will use to satisfy these requirements.

The contractor shall implement cybersecurity best practices to protect the IDE system and data pursuant to the level of the highest level of classification of the information contained within the IDE.

C.5.1.15 SUBTASK 15 – TRANSITION-IN

The contractor shall update the draft Transition-In Plan (**Section F, Deliverable 25**) provided with its proposal and provide a final Transition-In Plan as required in Section F (**Section F, Deliverable 26**). In the Transition-In Plan, the contractor shall account for all PL RCAS-FMS systems being transitioned-in and the anticipated timeline of the transition for each system. There shall be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan NLT ten calendar days after award. The Transition-In shall be completed in 60 days. All RCAS transition activities shall be completed 30 calendar days after approval of the final Transition-In Plan. All FMS and DRRS-A transition activities shall be completed 30 days after the RCAS transition.

C.5.1.16 SUBTASK 16 – TRANSITION-OUT

The contractor shall provide a Transition-Out Plan that facilitates the accomplishment of a seamless transition from the incumbent to incoming contractor and Government personnel at the

expiration of the TO. The contractor shall provide a Transition-Out Plan (**Section F, Deliverable 27)** NLT 90 days prior to expiration of the TO period. The contractor shall identify how it will coordinate with the incoming contractor and Government personnel to transfer knowledge regarding the following:

a. Program management processes.
b. POCs.
c. Location of technical and program management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall establish and maintain effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings.

Upon delivery of the final version release or other deliverable, the contractor shall deliver to the FEDSIM Contracting Officer's Representative (COR), the following:

a. All framework, source code (fully compliant package), libraries, database tables, scripts, resources, modules, and all other related materials on the Government system and all software code.
b. All procedures to move modules to test/production environments, maintenance procedures, reference materials, technical documentation, user manuals, training and/or classroom materials, and all other related documentation.
c. Documentation including system architecture diagrams, CM procedures (including creating new modules, modifying code, testing, checking in and out modules, production releases, version control, etc.), System Administrator (SA) procedures, database structure documentation, and data dictionary.

C.5.1.17 SUBTASK 17 – PREPARE TECHNICAL DIRECTION PLANS

The contractor shall prepare Technical Direction Plans (TDPs) in response to Government provided Technical Direction Letter (TDL) IAW **Section H.19**. The contractor shall tailor the requirements for each TDP. The TDP is an evolutionary document and the contractor shall work from the latest Government-approved version of the TDP.

The TDP shall include:

a. Project overview.
b. Project cost estimate (Rough Order of Magnitude (ROM)).
c. Master Equipment List (MEL)/Bill of Materials (if applicable).
d. Project schedule including milestones, tasks, and subtasks required in this project.
e. Project risks and mitigations.
f. Project staff and resources.
g. Performance criteria.
h. Travel considerations.
i. Project work products deliverables.
j. Security considerations.

k. Provide for an overall WBS.
l. Project transition.
m. TDP customer feedback participation.

The contractor shall host a Project Kick-Off Meeting for each approved TDL and shall provide a meeting agenda and meeting minutes.

C.5.2 TASK 2 – SOFTWARE ENGINEERING

The contractor shall establish a comprehensive software engineering program that rapidly deliver secure and working product and software solutions. The contractor shall provide a software engineering program that applies all relevant fields of engineering to include physical systems, requirements, design, development, testing, deployment, management of software systems across the RCAS-FMS portfolio.

The contractor shall establish software development lifecycle and engineering processes and organize for development and operations based on the Agile methodology. In furtherance of implementing Agile, the contractor shall establish a DevSecOps pipeline that builds in security and maximizes the concept of CI/CD that automates build, integration, and testing processes. The software engineering program shall enable an iterative approach to design, development, test, and implementation. The contractor shall develop a Product Development Life Cycle (PDLC) plan **(Section F, Deliverable 28**) and Software Development Life Cycle (SDLC) plan **(Section F, Deliverable 29**) that describes the end-to-end and detailed management approach. As part of the Software Engineering task, the contractor shall:

a. Establish an organizational structure and cross-functional teams to support all efforts.
b. Establish domain expertise in PL RCAS-FMS functional areas to understand the needs of stakeholders and develop an adaptive stance to manage change; in particular, the full range of operations across the Army Force Management Model which includes Total Army Analysis (TAA) and Programming, Planning, Budgeting, and Execution (PPBE), application of GFM DI in the Army, Global Force Management (Joint Publication 1-02), and the concepts of Dynamic Force Structure (DFS), Dynamic Force Employment (DFE), and Deploy to Redeploy (D2R).
c. Establish an enterprise design to identify and implement the “as-is,” “transitory,” and the “to-be” states to realize the PL RCAS-FMS requirements.
d. Sustain current (legacy) RCAS-FMS products (systems and infrastructure solutions) until they are subsumed, modernized, decommissioned, or as they are needed by the functional community.
e. Facilitate the transition of RCAS-FMS products from the “as-is” state to the “to-be” end state in ERPs. For RCAS, transition PER functionality to IPPS-A, transition SOH functionality to ASOHEIMS, and transition FA and MOB capability to FMS. For DRRS-A, transition capabilities to other systems For FMS, consolidate capability into the AOS/AOS DI framework.
f. For RCAS-FMS Products without a defined “to-be” state, establish a collaborative working relationship with the Government and functional proponents to develop and implement an appropriate end state for the entire RCAS-FMS portfolio.

g. As the portfolio's "to-be" state, enable PL RCAS-FMS to deliver an enterprise force management capability to support follow-on requirements in support of the HQ DA G-3/57 GFIM CMO.
h. Manage the evolution of underlying, disparate, and distributed RCAS-FMS infrastructure solutions to an enterprise solution IAW DoD guidance for Cloud and Application Migration and Consolidation.
i. Manage the consolidation of capabilities that currently exist outside the direct scope of PL RCAS-FMS but that are under the purview of the HQ DA G-3/5/7 GFIM CMO by executing learning, analysis, and design tasks in collaboration with mission partners in Government and in Industry.
j. Manage the data layer of supported systems by executing and nesting with efforts such as data cleansing. Examples of data efforts include supporting the Army Modeling and Simulation (M&S) Unified Data initiative, implementation of the GFM DI standard (see DoD Manual (DoDM) 8260.03 Volume 1 and Volume 2), and compliance with the Joint Requirements Oversight Council (JROC).
k. Establish a measurement method to enable PL RCAS-FMS to qualitatively and quantitatively understand and make informed decisions on quality, cost, schedule, and performance.
l. Deliver and manage a set of artifacts and data to enable full auditability.
m. Utilize commercial items and processes.

The contractor shall develop documentation and artifacts including:

a. Configuration Settings Document (CSD) (**Section F, Deliverable 30**).
b. Application Release/Service Pack Technical Information Packages (TIP) (**Section F, Deliverable 31**).
c. Release Plans (**Section F, Deliverable 32**).
d. Software User Manual (SUM) and ReadMe (**Section F, Deliverable 33**).
e. Database Administration Guide (DAG) (**Section F, Deliverable 34**).
f. System User Documentation – Web Administration Guide (WAG) (**Section F, Deliverable 35**).
g. Functional Requirements Document (FRD) - (**Section F, Deliverable 36**).
h. Requirements Traceability Matrix (RTM) - (**Section F, Deliverable 37**).

C.5.2.1 SUBTASK 1 – SYSTEMS ANALYSIS

The contractor shall provide systems analysis consisting of design, planning, and analysis that identifies technologies and processes to enhance the PL RCAS-FMS suite of applications, capitalizing on advancements in software development, automated testing, release methodologies, managing external interfaces, cyber security, mobile computing, data storage, and hosting environment to include cloud migration. At a minimum, the contractor shall utilize the following criteria: availability, maintainability, expandability, reliability, and conformance to Federal functional, security, and budgetary requirements.

The contractor shall include provisions for technology refreshes that will capitalize upon emerging technological advances available in commercial product offerings in its design concepts.

The contractor shall provide Systems Analysis documentation (**Section F, Deliverable 38**). At a minimum the Systems Analysis documentation shall contain:

a. Resources required to implement analysis.

b. Impacts to interface partners (internal/external).

c. Courses of Action (COA).

d. Results, findings, and providing recommendations.

e. Implementation plans.

f. Real-time Integrated Data Environment for Government review and feedback.

g. Rough Order of Magnitude (ROM).

The contractor shall conduct and provide assessment (**Section F, Deliverable 39**) of the PL RCAS-FMS enterprise environment. The contactor shall notify the PL RCAS-FMS TPOC and FEDSIM COR on cross-cutting architecture and technical issues that may impact the enterprise. At a minimum, the contractor shall provide:

a. Analysis of the existing operational state of the production environment to determine overall stability and reliability and identify vulnerabilities.

b. A detailed review, recommendation, and improvements of the system software, including its strength and weakness, in conformance with DoD and Army goals and initiatives and Best Business Practices (BBPs), and an overview of the reliability, security, availability, and portability.

c. Update the following standard DoD Architectural Framework (DoDAF):

    1. AV-1 Overview and Summary Information
    2. AV-2 Integrated Dictionary
    3. CV-1 Vision
    4. CV-2 Capability Taxonomy
    5. CV-3 Capability Phasing
    6. CV-4 Capability Dependencies
    7. CV-5 Capability to Organization Development Mapping
    8. CV-6 Capability to Operational Activities Mapping
    9. CV-7 Capability to Services Mapping
    10. OV-1 High Level Operational Concept Graphic
    11. OV-2 Operational Resource Flow Description
    12. OV-4 Organizational Relationships Chart
    13. OV-3 Operational Resource Flow Matrix
    14. OV-5 Operational Activity (Tree and Model)
    15. PV-2 Project Timelines
    16. SV-1 System/Services Interface Description
    17. SV-8 System Evolution Description
    18. SdtV-1 Technical Standards Profile

C.5.2.2 SUBTASK 2 – REQUIREMENTS MANAGEMENT

Requirements management support shall include documenting, sequencing, and tracing functional requirements. The contractor shall deliver and maintain a requirements management process acceptable to the PL RCAS-FMS to manage and account for changes in the systems requirements.

The contractor shall execute an enterprise requirements management program that enables the engineering and development process to deliver functionally relevant capability while providing PL RCAS-FMS with sufficient artifacts to audit the requirements lifecycle.

The contractor shall update documentation such as Context Diagrams, Use Case Models, Business Process Models (BPM), and associated design documentation for new requirements and iterations of an application system IAW applicable DoD standards. The contractor shall assess and document the impact of new functional requirements on the existing design baseline.

The contractor shall implement changes to the baseline IAW a rigorous CM process, which is currently tracked by the ECP process through the TDL process (see **Section H.19**). The ECP process generally includes the infrastructure to efficiently accept new requirements with visibility and transparency through completion. The Government expects this process to be timely and thorough and have no impact on other software-related activities.

The contractor shall maintain that any changes to the application design are in conformance with the Human Factors Engineering of Computer Workstations ANSI/HFS 100-2007.

The contractor shall execute a Requirements Management Program, which will facilitate the following:

a. Support projects with varying degrees of requirements stability from clearly defined to unprecedented to rapidly changing.
b. Support adaptive planning, evolutionary development, early delivery, and continual improvement for all aspects of the program.
c. Provide the Government flexibility for implementing changing requirements to the baseline, as they occur.
d. Allow the Government to meet, possess, and manage artifacts required to meet audit benchmarks (i.e., cyber Risk Management Framework) Government audits.
e. Leverage automation to the maximum amount possible to capture, define, assess, and implement requirements with transparency and efficiency.
f. Allow the Government to comply with applicable Defense Acquisition regulations and policies regarding risk management.
g. Determine the impact on any internal/external system(s).
h. Execute technical leadership and coordination meetings with Government leads and interface partners.

C.5.2.3 SUBTASK 3 – SOFTWARE DEVELOPMENT

The contractor shall execute software development to deliver secured and working software rapidly, incrementally, and continuously in keeping with Agile best practices. The contractor shall develop software that enables simplicity/ease of use and reduces the burden on user training and documentation.

The contractor shall produce the SDP to demonstrate how software development nests with the Product Development Life Cycle (PDLC), SDLC, and all applicable International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) standards.

As outlined in the SDP (**Section F, Deliverable 4**), the contractor shall identify and execute:

a. A lifecycle model that leverages innovative and holistic solutions within a flexible, adaptive methodology.
b. Primary and supporting organizational processes based on the work content of this performance work statement.
c. The management, composition, structure, and responsibilities of cross-functional teams.
d. A process in which the contractor and Government will work together in support of software development.
e. Activities to be performed as a part of the processes, tasks that support the activities, and techniques and tools to be used.
f. How the contractor will implement supporting processes and programs (e.g., test, cybersecurity, QA, risk management, automation, software/hardware integration, version control, release management) and include and leverage the automated tools PL RCAS-FMS has made investments in and that are mandated by higher headquarters.
g. Specific standards, methods, tools, commercial items, actions, strategies, and responsibilities associated with development and testing.
h. An enterprise training plan focused on providing all stakeholders (i.e., Government Program Management Office (PMO), functional proponents, mission partners) with a thorough understanding of the contractor's software development methodologies and testing tools and processes.
i. New technology based on analysis of current trends in order to adapt to industry best practices and develop periodic technology refresh and enhancement plans.
j. Technical/management leadership of analysis of highly specialized applications and operational environments, functional systems analysis, design, integration, documentation, and implementation of technical solutions.

C.5.2.4 SUBTASK 4 – DATABASES

The design, development, management, and sustainment of data and databases in the PL RCAS-FMS portfolio of systems are critical to fielding operational software. The contractor shall:

a. Administer databases and incorporate changes or updates to the supporting data models, schemas, data dictionary, and related support software to manage both the development and production database environment.
b. Provide continuous improvement to the integration of the information within the database to facilitate data sharing across the applications.
c. Adhere to and remain abreast of Government data standards in order to ensure full compliance with Government data standards.
d. Maintain and enhance the integrated database to support the data storage requirements.
e. Develop an enterprise approach to managing disparate database solutions in order to leverage commercial expertise.

C.5.2.5 SUBTASK 5 – INFORMATION EXCHANGES (IE)

IE represents the inbound and outbound connection between systems. The contractor shall:

a. Facilitate the rapid and secure exchange of information, both internally and externally.
b. Provide a standardized, enterprise approach to managing IE.
c. Design, develop, and implement automated IE, to the greatest extent possible.
d. Analyze, coordinate, and develop technical solutions, defined by the requirements, for all IE.
e. Monitor changes to and sustainment of the existing IE.
f. Maintain technical specifications and incorporate changes or updates to the software and documentation (**Section F, Deliverable 40**).

C.5.2.6 SUBTASK 6 – TESTING

The contractor shall provide testing that is holistically integrated into the program's engineering, QA/quality management, and development processes for rapid deployment of working software and reduce defects and rework.

Testing requires frequent engagement with the end-user community and designated representatives (proxies, testers). Development and testing shall include use of automated regression test techniques as part of a CI/CD process. The contractor shall, at minimum:

a. Thoroughly test all products, to include maximum use of automation, smoke tests, regression testing, and stress and boundary testing. The contractor shall identify and correct all product issues throughout the software development process, the contractor shall identify and correct product test issues.
b. Conduct appropriate tests consistent with the developmental methodology (e.g., unit, functional, system, interoperability, regression, security, and performance) of software throughout the development lifecycle.
c. Maintain test materials (e.g., scripts, configurations, utilities, tools, plans, and results) under configuration control.
d. Develop and deliver test procedures, test data, materials, results, and artifacts (**Section F, Deliverable 41**) in a format that allows the Government to reproduce the test within its own test environment. The Government will provide only one instance of test data. The contractor shall maintain and update this one provided instance of the test data for future use; the Government will not provide any other instances of test data.
e. Conduct tests related to non-functional requirements (e.g., load, performance and installation testing).
f. Correct software defects throughout the software development process identified through testing including unit, system, functional, security, performance, and load testing procedures.
g. Document systems and application performance and load data as part of the testing process (**Section F, Deliverable 42**). The contractor shall make this data available to the Government upon request.
h. Provide support for the Government's validation testing.
i. Include the PL RCAS-FMS TPOC as part of the iteration tests/demonstrations.

Test scripts, utilities, execution, and results shall be historically maintained under configuration control for comparison and analysis and delivered to the Government.

C.5.2.7 SUBTASK 7 – TEST ENVIRONMENT

The contractor shall sustain an enterprise test environment that is representative of all production environment systems in order to facilitate Government-specific test and validation requirements, training, and evaluation.

Upon delivery of source codes, build materials, and related artifacts by the contractor to the test environment, source code evaluation and scanning, installation instructions, and testing (e.g., functional, security, load, performance, etc.) will be conducted within the test environment. The contractor shall address any issues encountered during installation of test media, test execution, or resolve any problems with the applications.

The contractor shall provide media (**Section F, Deliverable 43**) for all source code, installation kits, software, and documentation including those related to architecture, test design and test results, and installation procedures, and build procedures/scripts in a secure manner at the end of each update.

The contractor shall document in the SDP third-party products used to develop, operate, and construct the software applications.

C.5.2.8 SUBTASK 8 – SOFTWARE DEPLOYMENT MANAGEMENT

The contractor shall develop a software deployment roadmap that encompasses the individual detailed project plans.

The software detailed project plans shall include the following minimum content:

a. Software Version Description Document that includes the content of each update and any known limitations.
b. Unique identifiers for each update.
c. Installation instructions and update media.

The contractor shall develop and implement an integrated software deployment management solution that reduces the implementation burden on units in the field.

The contractor software deployment management practices and processes shall be complementary to Government practices and processes.

C.5.3 TASK 3 – IT INFRASTRUCTURE AND NETWORK ENGINEERING

The contractor shall provide a broad range of IT engineering and integration services to deliver administration (e.g., systems and database), infrastructure (e.g., physical and virtual), and networking (e.g., routing and switching) solutions in support of the PL RCAS-FMS and its supported applications and client organizations. The contractor shall provide the entire IT engineering lifecycle from requirements gathering, system design and development, installation, integration and testing, and operations and sustainment. The contractor shall develop and maintain a Systems Engineering Plan (SEP) and a Systems Engineering Management Plan (SEMP) (**Section F, Deliverables 44 and 45**).

C.5.3.1 SUBTASK 1 – CLOUD MIGRATION

The contractor shall provide cloud migration, consolidation, and rationalization IAW DoD/Army directives and standards. As required, the contractor shall migrate RCAS-FMS PO systems to the cloud, which includes designing a solution, procuring the service if necessary, and continuing to work with the approved cloud service provider pursuant to service providers identified in Army Cloud Computing Enterprise Transformation (ACCENT) or with the best available DoD-compliant commercial providers.

The contractor shall evaluate available hosting solutions to meet the program requirements. When a hosting environment is selected, the contractor shall design and migrate PL RCAS-FMS PO PROD infrastructure to a consolidated or centralized location that is compliant with the DoD and Army Standards and accounts for the needs to work on NIPR and SIPR as required. The Contractor shall perform the decommissioning of legacy hardware, licensing, and maintenance support agreements after the migration has occurred. The contractor shall design and execute the migration of RCAS, FMS, DRRS-A, and IMA/ARNG DEV and TEST environments to a single cloud solution as part of the contractor environment as identified in **Section H.15.2**.

The contractor shall take into account the system evolution of the supported applications including the current and future state when identifying and planning migration efforts.

C.5.3.2 SUBTASK 2 – EXTERNAL HOSTED OPERATIONS

The contractor shall provide system administration and database administration to sustain external operations of all PL RCAS-FMS major program areas. The degree of administration varies depending on the specific configuration of each environment. In instances where the RCAS-FMS program is not directly responsible for managing systems within the hosting environment, the PL RCAS-FMS TPOC and/or the FEDSIM COR will facilitate contractor coordination directly with the provider (i.e., data center or cloud provider) to ensure the consistently reliable operational availability of RCAS-FMS capabilities (see **Section J, Attachment F**, Current IT and Network Environment).

The contractor shall support the RCAS operational environment at Fort Bragg, North Carolina (NC), which is currently hosted by the USARC UCS pursuant to an Service Level Agreement (SLA) between the USARC G6 and PL RCAS-FMS to host RCAS-FMS production and training environments in support of the RCAS-FMS ARNG and RCAS-FMS USAR communities.

The contractor shall support the FMS operational environment at the Army Data Center Fairfield Enclave (ADCF-E) which is operated by the Army Analytics Group (AAG) pursuant to a

Support Agreement between AAG and PL RCAS-FMS and as further described by the current System Security Plan (SSP) to host FMS development, test, and production environments.

The contractor shall support the DRRS-A operational environment that hosts DRRS-A development, test, and production environments. The contractor shall support the transition of the DRRS-A operational environment and associated needs to OSD as directed by the Government.

At a high-level, the contractor shall:

a. Execute all RCAS-FMS responsibilities as a tenant specific to each program area and coordinate through the division of responsibilities with the host provider.
b. Support the RCAS-FMS mission pursuant to the local Command (protocols, policies, procedures) during regular business hours defined as 7:00 a.m. to 5:00 p.m. Eastern Time (ET), excluding weekends and Federal holidays.
c. Conduct operations and maintenance of servers and applications as applicable (e.g., production, staging, Continuity of Operations (COOP) Plan, and training/test servers).
d. Ensure the availability and reliability of applications and integrity of databases.
e. Serve as the singular coordination point between the RCAS-FMS PO and each hosting provider.

At a detailed-level for system administration and where applicable, the contractor shall:

a. Provide system administration expertise relevant to the supporting commercial solutions (e.g., VMWare) including design, implementation, maintenance, and repair.
b. Install applications and configure the O/S within the UCS environment.
c. Ensure all servers are Information Assurance Vulnerability Alert (IAVA) and STIG compliant.
d. Install/update O/S patches.
e. Perform security checklists on O/S and system backups for each server.
f. Perform daily server operations and maintenance.
g. Perform server troubleshooting.
h. Monitor system logs, security logs, and application logs.
i. Perform detailed monitoring and tuning.
j. Provide file transfer, archiving, data backup, and restoration.
k. Provide server and application operation and maintenance support for functional staff specific applications.
l. Perform daily training server operations and maintain and administer student accounts.
m. Develop processes and procedures.
n. Keep servers up to date with the most current fielded application baseline.

At a detailed-level for database administration and where applicable, the contractor shall:

a. Provide database administration expertise relevant to the RCAS-FMS database solution (e.g., Oracle) including design, implementation, maintenance, and repair.
b. Develop and design database strategies and monitor and improve database performance and capacity.
c. Plan, coordinate, and implement security measures to safeguard the database.

d. Install and upgrade the database server and application tools.
e. Allocate system storage and plan for future database storage requirements.
f. Create primary database storage structures (table spaces) after application developers have designed an application.
g. Create primary objects (e.g., tables, views, indexes) once application developers have designed an application.
h. Modify the database structure, as necessary, from information given by application developers.
i. Enroll users and maintain system security.
j. Ensure compliance with the database license agreement.
k. Control and monitor user access to the database.
l. Monitor and optimize the performance of the database.
m. Plan for backup and recovery of database information.
n. Backup and restore the database.
o. Coordinate with the database vendor for technical support.

C.5.3.3 SUBTASK 3 – TECHNICAL REFRESH AND HARDWARE AND SOFTWARE INTEGRATION

The contractor shall provide technical refresh and integration of hardware and software IAW **Section H.19**.

The contractor shall identify product end-of-life and support candidates, and evaluate submitted deviations and waivers.

The contractor shall manage, test, and install the items in the operational environment. The contractor shall configure, pre-assemble/assemble, integrate, prepare for shipment, and ship or install product components to designated locations.

The contractor shall provide processes and methodologies necessary to systematically deliver, install, and account for equipment to fully equip or retrofit sites designated by the Government. Installation may involve fabrication of mounts, brackets, and installation kits. The contractor shall inform the Facilities Maintenance Officer (FMO) on electrical power, space, and lighting requirements, as well as other architectural, logistical, and facility planning considerations.

The contractor shall provide IT support to operational sites (such as incident command centers) for items (e.g., monitors, data lines, and Video Teleconferencing (VTC) capability). The contractor shall coordinate the installation of equipment and all other contractor services, including site surveys, necessary to complete the installation for each of the designated sites.

C.5.3.4 SUBTASK 4 –ENGINEERING SUSTAINMENT

The contractor shall provide sustaining engineering to RCAS-FMS PO fielded systems. At a minimum, the contractor shall:

a. Provide Network components, telecommunication, and VTC equipment maintenance support.
b. Resolve escalated break-fix tickets on various IT components.

c. Conduct infrastructure analysis, designs, and implementation for new and existing environments.
d. Provide network trouble shooting for newly implemented networks.
e. Provide recommendations for replacement of end of life or near end of life for all hardware and software components.
f. Provide VTC expertise.
g. Sustain functionality of the complete family of in-service hardware and software products, and shall provide security and product updates, quality releases, patches, fixes, and service packs are installed IAW the manufacturer's recommendations.
h. Provide support for activities performed in support of equipment maintenance including ensuring repair of failed components, shipping replacement components (i.e., generating DD Form 1149), issuing/monitoring equipment manufacturer Return Material Authorizations (RMAs), procuring spares/maintenance equipment in support of field failures, establishing and tracking of equipment warranties, performing periodic equipment inventories, and providing equipment failure trend monitoring and analysis.
i. Maintain the Baseline and Hardware Matrices for all hardware and software under the RCAS FMS PO responsibility (**Section F, Deliverable 46**).
j. Conduct engineering studies (**Section F, Deliverable 47**) and analysis to support future system enhancements.
k. Support pre-implementation travel to observe conditions of sites to receive IT services.
l. Provide innovations support to improve current hardware operating environments that supports improvements or modernization.

C.5.3.5 SUBTASK 5 – IT INFRASTRUCTURE PLANNING AND DESIGN

The contractor shall provide analysis, planning, and design a complete Voice over Internet Protocol (VoIP) topology for the United States Army Reserves G6, which will ultimately be implemented to support new and existing Army Reserve Centers across the U.S. The solutions will be required to Integrate and be interoperable with existing USARC network topology.

The Government will provide GFI IAW **Section H.19**, Technical Direction Letter.

The Property Book Officer (PBO) (or Government designee per the DA For 1687) and contractor representative will perform a joint inventory of the equipment and sign the DD Form 250 (**Section F, Deliverable 48**) and, if necessary, the DD 1149.

At a minimum, the contractor shall:

a. Perform analysis, conduct designs, and recommended adjustments based on GFI data.
b. Allow for multiple site designs to be developed simultaneously IAW the list of sites provided by the Government.
c. Provide cost estimates including labor, travel, and Lists of Materials (LOM) to support data requirements at each site along with its associated network connectivity diagram.
d. Review and analyze supporting documents posted on websites.
e. Derive network designs from site-specific GFI and result in a complete solution.
f. Place appropriate consideration when augmenting or adding to existing networks related to outdated and end of life equipment.

g. Complete the design based upon assumptions and historical data, in lieu of any missing GFI data.
h. Accomplish site-specific equipment sizing using the GFI for the data network and, if required, voice network.
i. Develop site-specific equipment LOMs (**Section F, Deliverable 49**) to field the local area data network and, if required, voice network to implement the engineering design requirements.
j. Develop site-specific labor cost estimates to configure, test, ship, and install the hardware to implement the engineering design requirements.
k. Populate the Site Cost Estimate Worksheet and finalize all summary cost data.
l. Document the LOM within the Site Cost Estimate Worksheet and include network connectivity diagrams upon completion of each site's initial engineering design review process.
m. Support pre-implementation trips.
n. Conduct meetings, interact with key stakeholders, and provide updates, as required, on a by site bases.
o. Provide inside and outside plant activities, when required.

The contractor shall develop and provide Project Implementation Plan (**Section F, Deliverable 50**). The contractor shall provide personnel with appropriate certifications to accomplish inside and outside network services and be able to operate on Army networks. All personnel conducting implementation services for this task require access to military networks and elevated privileges. The contractor shall purchase the necessary equipment and tools, configure/test the equipment, ship the equipment to the project location, and conduct the network installation.

C.5.3.5.1 SUBTASK 5.1 – NETWORK INSTALLATION

The contractor shall purchase the necessary equipment and tools, configure/test the equipment, ship the equipment to the project location, and conduct the network installation IAW the design developed in **Section C.5.3.5**. The contractor shall ship equipment/tools to a specific site PBO as identified on the DA Form 1687. The site PBO will be identified prior to any shipment of equipment. The PBO will safeguard the equipment/tools at the site until the contractor's Installation Team arrives. Upon contractor arrival at the installation site, the PBO (or Government designee per the DA Form 1687) and contractor representative will perform a joint inventory of the equipment and sign the DD Form 250. The contractor shall execute IT Planning and design IAW **Section H.19.**

The contractor shall conduct the necessary testing to confirm operability; operability will be confirmed by an assigned (local) Government technical representative for the on-site IT network installation.

At a minimum, the contractor shall provide the following Deliverables IAW **Section H.19**:

a. Walk-Through Checklist (**Section F, Deliverable 51**)
b. Post-Installation Checklist (**Section F, Deliverable 52**)
c. Customer Satisfaction Questionnaire (**Section F, Deliverable 53**)
d. Test Procedure Checklist (**Section F, Deliverable 54**)

e. The contractor's delivery of "As Built Network Drawings" to Government CM (**Section F, Deliverable 55**)

As requested by the Government, the contractor shall conduct meetings with the PL RCAS-FMS in order to communicate project status and identify issues. The contractor shall prepare and submit Site Status reports (**Section F, Deliverable 56**). As necessary, the contractor shall attend regularly scheduled project coordination and status meetings in person with the staff of the military organization (e.g., USARC G2/G6 and the Assistant Chief of Staff for Installation Management (ACSIM) organizations). The contractor shall prepare and deliver meeting minutes (**Section F, Deliverable 57**) to record the results of these meetings.

C.5.4 TASK 4 – CYBERSECURITY

The contractor shall implement and maintain all aspects of cybersecurity engineering support IAW all Federal, DoD, Component, and Agency-specific security initiatives. The contractor shall implement all phases and aspects of the DoD accreditation/certification policies and procedures for DoD IT during the entire lifecycle for all systems and environments. The contractor shall evaluate, identify, and implement innovative cybersecurity practices and tools to enable the Government to meet security standards with the greatest possible efficiency.

The contractor shall develop a Cybersecurity Strategy Plan (**Section F, Deliverable 58**) that describes concisely how a program's cybersecurity features comply with applicable standards, regulations, and requirements. The Cybersecurity Strategy Plan shall briefly describe the system, the program's risk assessment in the face of cyber and physical threats, and the Assessment and Authorization (A&A) approach.

At a minimum, the contractor shall monitor and evaluate cybersecurity-related list services such as Information Assurance Support Environment (IASE) and Army Computer Emergency Response Team (ACERT) portal, and alerts/notifications from authoritative organizations such as Regional Cyber Centers (RCC), Defensive Cyber Operations (DCO), the U.S. Army Network Command (NETCOM), and Army Cyber Command (ARCYBER) to ensure the most current information is being utilized to maintain a secure baseline.

The contractor shall develop and maintain a program Enterprise Architecture and Technology Roadmap by incorporating evolving cybersecurity requirements and emerging technologies to comply with the DoDAF.

The contractor shall provide and maintain a CSD that describes how vulnerability is resolved or mitigated (**Section F, Deliverable 30**).

The contractor shall develop and maintain an automated Cross Domain Enterprise Solution (CDES) for the synchronization of data from SIPRNet to NIPRNet and vice versa.

The contractor shall acquire commercial items for security functions (excluding cryptographic modules) IAW policies and guidance contained in the DoD IT Standards and Profile Registry (DISR), https://disronline.csd.disa.mil/, which requires a CAC for access.

The contractor shall assess the program's systems against changes to published or known vulnerabilities such as STIGs and Cybersecurity Vulnerability Management (CVM) alerts/bulletins and implement mitigation strategies.

The contractor shall maintain that the program meets requirements for certificate-based authentication (i.e., CAC and Public Key Infrastructure (PKI)) and integration with U.S. Army enterprise authentication policies, procedures, and systems.

The contractor shall address the cybersecurity ramifications that are associated with any system change.

The contractor shall maintain that all systems meet authorization requirements set forth by Government Cybersecurity personnel, the accreditation/certification process, and Connectivity or Interconnectivity activities as required, including providing cybersecurity artifacts/documentation, upon request, in a format acceptable to Government.

The contractor shall establish an integrated cybersecurity program for all phases of the SDLC during the execution of this program IAW at least the following key references:

a. NIST publications and guidance (https://www.nist.gov/).
b. DoD Directive (DoDD) 8140, Cybersecurity Workforce Management (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf).
c. DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD IT (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf).
d. DoDM 8570.01-M, Cybersecurity Workforce Improvement Program (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf).
e. Army Regulation (AR) 25-1, Army Information Technology (https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r25_1.pdf).
f. AR 25-2, Information Assurance (https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r25_2.pdf).
g. Component and Agency level authoritative references.
h. Industry standards and best practices.

The contractor shall obtain and maintain the program's Authorization to Operate (ATO) accreditation activities IAW current DoD policy.

Assess Only (AO) requirements shall be IAW current DoD policy.

C.5.4.1 SUBTASK 1 – CYBERSECURITY OPERATIONS

The contractor shall develop, document, and execute CsMPs, SOPs, and processes as a means to demonstrate compliance with and implement security controls. The following list identifies the minimally expected documents or topics to be included:

a. Cybersecurity Strategy.
b. CsMP.
c. Vulnerability Management Plan (VMP).
d. STIG Assessments.
e. STIG Assessment Process.
f. CSD.
g. CSD Change Process.
h. Software Assurance and Quality Scanning Process (Development).

i. Software Assurance and Quality Scanning Process (Production).
j. Ports, Protocols, and Services (PPS).
k. Cybersecurity Threat Models.
l. Cybersecurity Threat Modeling Process.
m. Incident Response Plan (IRP).
n. COOP and Disaster Recovery (DR).
o. Security Accreditation Architecture Diagram.
p. Whitelisting Procedures.
q. Army Registry of Networks and Layer-3 Devices (ARNLD).

The contractor shall develop and maintain a Privacy Impact Assessment (PIA) for each system (**Section F, Deliverable 60**).

The contractor shall maintain a high state of Cybersecurity compliance and operational availability by monitoring and applying all applicable STIGs and patches within the mandated implementation period for PL RCAS-FMS instances at the USARC UCS located at Fort Bragg, NC maintain a

The contractor shall execute a continuous monitoring program by conducting cybersecurity audits based on NIST and RMF controls such that 100 percent of the cybersecurity controls that are applicable to the program are audited over a three-year period; annually, the contractor shall audit at least 33 percent of controls and ensure that the results are integrated into the program's eMASS record for implementation, compliance, and reporting purposes.

The contractor shall apply for and maintain AO, where applicable, pursuant to NETCOM and ARCYBER guidance (**Section F, Deliverable 61**).

The contractor shall utilize the Army Training and Certification Tracking System (ATCTS) to manage training and certifications for personnel performing cybersecurity duties. The contractor shall request appointments by filling out the Appointment Orders form(s) (https://atc.us.army.mil/iastar/login.php) and shall maintain ATCTS user accounts by keeping user information current, including certifications and personnel info. The contractor shall provide personnel accessing information systems with the proper and current information assurance certification to perform information assurance functions IAW DoD 8570.01-M, Information Assurance Workforce improvement Program.

At a minimum, the contractor cybersecurity controls shall include:

a. Enable all systems to address all systems controls, and execute A&A and re-authorization activities IAW DoDI 8500.1, DoDI 8510.01, NIST SP 800-53, and CNSSAM TEMPEST/01-13.
b. Establish secure baseline configurations IAW DISA STIG, Information Assurance Vulnerability Management (IAVM) notices, AR 25-1, AR 25-2, AR 380-5, and NIST SP 800-53; where applicable, apply security controls for Secret Internet Protocol Router Network (SIPRNet) and NIPRNet enclaves. Continuously evaluate the system's security posture to ensure that the program is meeting goals, that system patches are up-to-date, and that security controls are still effective. Actively maintain and execute a POA&M to mitigate system vulnerabilities for all systems baselines and for all PM-controlled environments and systems.

c. Utilize the DoD system of record to manage the systems' current accreditation; the current system of record is the Electronic Mission Assurance Support System (eMASS). The contractor shall be the Information System Security Officer (ISSO) for eMASS. eMASS is the program of record that automates a broad range of services for comprehensive, fully-integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of RMF for DoD IT.
d. Reference the RMF Knowledge Service web site as the DoD's' official site for enterprise RMF policy and implementation guidelines and is a useful source of information. The web site provides tools for selecting controls under RMF, including Controls Explorer. Access to RMF Knowledge Service requires a CAC/DoD PKI certificate and one-time registration at https://rmfks.osd.mil/login.htm.
e. Develop, maintain, and address security concerns in applicable MOAs, MOUs, SLAs, and ISAs to ensure that all systems meet security requirements throughout the whole life-cycle.
f. Ensure that all systems meet FISMA compliance for Contingency Test, Security Control Test, and Annual Security Review.
g. Manage security and policy requirements pertaining to the use, protection, and reduction of PII; support Privacy Impact Assessment (PIA) or System or Record Notification (SORN) requirements.
h. Integrate and manage scanning and patching processes as they relate to DoD and DA accepted software to ensure software assurance, vulnerability management, and software quality.
i. Manage security requirements pertaining to DISA STIGs, IAVMs, and related notices and issuances from U.S Army Cyber (ARCYBER), U.S. Cyber Command (USCYBERCOM), the ARNG, and USAR.
j. Leverage current technologies, to automate resource intensive processes such as scanning, vulnerability analysis, reporting, and patch management.
k. Establish a reporting process to inform FEDSIM COR and RCAS-FMS TPOC to allow the Government to make informed decisions.
l. Provide cybersecurity reports (e.g., raw scan results, scan analysis, and general status reporting on a periodic basis or ad-hoc basis as conditions dictate).
m. Ensure that all PM-controlled systems and environments meet scanning, patching, and operational requirements as dictated by their respective commands.

C.5.4.2 SUBTASK 2 – CYBERSECURITY DESIGN

The contractor shall incorporate cybersecurity BBPs into its engineering design as a component of the system design. The contractor shall document the criteria for a cyber-resilient engineering design in the SDP.

All cyber/cyber-enabled equipment specified in the design plan must be Joint Interoperability Testing Command (JITC) compliant, found on the DoD Unified Capabilities Approved Product Lists (UC APLs) established IAW the UC Requirements (UCR 2013) document and mandated by DoDI 8100.04. The contractor shall maintain the hardware and software inventory to be in compliance with the UC APL in the SDP.

All system components specified in the design plan must be capable of configuration IAW the DISA STIG and Army BBPs. System configuration includes applying IAVA/Information Assurance Vulnerability Bulletin (IAVBs) and STIGs (manual and automated) individually without the need to re-image the system and during new capability updates.

If the contractor's design includes components or software that are not on the UC APL or does not have an AO, contractor shall provide support in obtaining UC APL acceptance or an AO. The contractor shall maintain that the hardware/software inventory is in compliance with the UC APL and U.S. Army AO for all software in the SDP.

The contractor shall submit and collect the AO application required by NETCOM for the applications, systems, networks, and/or information systems. The contractor shall follow NECOM AO instructions.

The contractor shall format all architecture diagrams and demonstrate adequate security controls compliant with the most up to date version of the DoDAF format.

The contractor shall document and provide to the Government all deviations and otherwise non-compliance with applicable STIGs, CVMs, or other security configurations and patches to show what settings and patches could not be applied and the rationale for not applying the configuration/patch. Maintaining may include CM of system baseline documentation as applicable and submission and approval of change requests to the appropriate change control body before changes are made to those systems.

C.5.4.3 SUBTASK 3 – SECURE BASELINE CONFIGURATION AND VULNERABILITY MANAGEMENT

The contractor shall provide an enterprise process for Verification and Validation activities, at a minimum: assess, evaluate, analyze, and report the results of compliancy testing of STIG items and to provide automated compliance reporting for STIGs.

The contractor shall provide patching, system hardening, and fixing/mitigating findings from vulnerability scan results or manual assessments. The systems shall be hardened using the required and approved STIGs, Security Requirements Guides (SRGs), and Security Content Automation Protocol (SCAP) Benchmarks.

The contractor shall implement a secure and compliant standardized baseline configuration on every instance of every type of device fielded IAW DISA and U.S. Army guidelines.

The contractor shall implement STIGs within 30 days from release of a new DISA STIG. The systems shall be patched IAW DISA and U.S. Army guidelines.

The contractor shall analyze the vulnerability scan results including non-compliant findings. The contractor shall utilize the vulnerability scanning tool and execute the vulnerability scans using a U.S. Army approved method (e.g., Assured Compliance Assessment Solution (ACAS)).

The contractor shall provide Cybersecurity Test Results (**Section F, Deliverable 62**), demonstrating a secure and compliant baseline configuration including the following:

a. Analysis of Vulnerability Scans.
b. Manual Assessments.
c. DISA STIG Checklists IAW local Cybersecurity guidelines.

d. Compliance Report.
e. Systems Hardening Analysis Report.
f. POA&M.
g. Software Code Assurance Assessment.

C.5.4.4 SUBTASK 4 – COOP SUPPORT

The contractor shall maintain a COOP Plan in compliance with FISMA supporting and reporting activities (**Section F, Deliverable 63**) for the systems and operating environments within the scope of control of this program that minimally include the development environment, contractor's facility, and production environments.

The contractor shall support COOP activities at the systems' COOP locations in the event that COOP is implemented and services are moved to the COOP location. Contractor support shall involve assisting in the performance of the responsibilities, hosting facility site personnel including SA/Database Administrator (DBA) responsibilities. The contractor shall maintain COOP servers at the proper RCAS-FMS update level and that all cybersecurity controls are in place.

The contractor execute specific duties/responsibilities and alternate work locations outlined in SOPs, MOAs, and RCAS-FMS COOP documentation.

The contractor shall maintain PL RCAS-FMS instances at the hosting facility site at a high state of Cybersecurity compliance and operational availability by monitoring and applying all applicable STIGs and patches within the mandated implementation period.

In addition, the contractor shall:

a. Evaluate software application issues on site and in the field.
b. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
c. Apply all applicable software patches/upgrades IAW cybersecurity process.
d. Coordinate and install all program releases in coordination with COOP site outage schedules.
e. Troubleshoot end-user issues/trouble tickets as applicable.
f. Effectively communicate issues and resolutions to all levels of the organization.
g. Interact with internal and external customers.
h. Ensure that all applicable IEs are updated to point to servers in the event COOP is activated.
i. Participate in COOP-related training and exercises.
j. Produce innovative solutions for a variety of complex problems.
k. Identify alternatives and implications of a newly revised system.
l. Identify omissions and errors in requirements and recommend best practices.
m. Plan work schedules and perform customer support activities involving software design, developments, testing, and program management.

C.5.5 TASK 5 – ENTERPRISE HELP DESK SUPPORT

The contractor shall provide Tier 2 and Tier 3 Enterprise Service Desk support that shall include telephonic and on-site support. Tier 1 support will be supported outside of this TO through a combination of Army Enterprise Service Desk (AESD), the AESD NG, and the Army Reserve Help Desk. The contractor shall identify customer problems and implement repeatable, best practice solutions across the enterprise.

The following are representative tasks performed at each support level:

a. Tier 2 Support – The contractor shall provide Tier 2 support level for customers. Tier 2 Support will receive tickets from the Tier 1 team. Tier 2 support shall provide users with more complex support and subject matter expertise on supported software applications including hardware and software technical assistance and service requests from the Tier 1 level. The contractor shall escalate Tier 2 ticket to Tier 3 level requiring further assistance.
b. Tier 3 Support – The contractor shall provide more advanced technical support on highly complex inquiries and support on critical calls that may have an immediate, negative impact on operations. The contractor shall address technical issues that cannot be resolved at lower tiers of the Enterprise Help Desk.

C.5.5.1 SUBTASK 1 – TIER 2 SUPPORT

The contractor shall provide the following:

a. Identify customer problems and solutions and maintain corrective procedures that are repeatable across the enterprise.
b. Review, modify, and develop standards and procedures for the problem resolution process (**Section F, Deliverable 64**), which includes focusing on customer call reduction and the use of root cause analysis. The contractor shall create and maintain updated online information about known root causes, symptoms, and resolutions.
c. Perform Tier 2 field support.
d. Monitor the problem resolution processes.
e. Measure performance and analyze data to isolate and solve computing, security, and networking problems.
f. Monitor the problem resolution process from initial contact to post-resolution, end-user feedback.
g. Provide live coverage from 7:00 a.m. to 5:00 p.m. ET, excluding weekends and Federal holidays.

C.5.5.2 SUBTASK 2 – TIER 3 SUPPORT

The contractor shall respond and address technical issues that cannot be resolved at lower tiers of the Enterprise Help Desk. This support shall include remote and on-site system engineering support for RCAS-FMS projects, fielded commercial items, and hardware issues.

The contractor shall provide the following:

a. Evaluate software application issues onsite.

b. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
c. Effectively communicate issues and resolutions to all levels of the organization.
d. Interact with internal and external customers.
e. Produce and document innovative solutions for a variety of complex problems.
f. Identify alternatives and implications of a newly revised system.
g. Identify omissions and errors in requirements and recommend optimum approaches.

C.5.6 TASK 6 – TRAINING

Training is a critical component of ensuring all users are capable of operating the hardware and software aspects of the projects under the PL RCAS-FMS. The contractor shall deliver an enterprise training solution that provides training and education requirements to support PL RCAS-FMS. Training will be provided for the PL RCAS-FMS portfolio.

The contractor shall be prepared to conduct training on software updates upon Government acceptance.

The contractor shall conduct classes IAW all applicable Training and Doctrine Command (TRADOC) standards. The contractor shall conduct classes on all applications at a variety of sites such as the Professional Education Center (PEC), Little Rock, Arkansas (AR), the Army Reserve Readiness Training Center (ARRTC), Fort Knox, Kentucky (KY), and other end user locations within the RCAS-FMS portfolio.

The following is a list of minimum tasks the contractor shall perform in order to produce Training online and instructor lead opportunities that will support current and future operations of all projects under the RCAS-FMS portfolio:

a. Develop and maintain an Enterprise Training Plan (**Section F, Deliverable 65**).
b. Maintain all applicable documentation, including delivery methods, user documentation, and current training materials.
c. Coordinate with and support Training Centers such as TRADOC, the Force Management Support Agency (FMSA), PEC, and other military training organizations and efforts that PL RCAS-FMS supports throughout all three Army Components.
d. Deliver the enterprise training capability such that the end users of PL RCAS-FMS systems understand how to use RCAS-FMS Products and that the entire RCAS-FMS organization understands how to operate as a team to deliver these products.
e. Develop media such as training and educational videos in concert with product releases (**Section F, Deliverable 66**), as required.
f. Maintain training, educational, and representative systems in compliance with all applicable DoD and Army Security Regulations.
g. Deliver subject matter expertise for the operational support and maintenance of the Training Servers including system security, systems monitoring, troubleshooting, repairs, performance evaluation, applying updates and patches, and creating student accounts for soldiers attending functional training. See **Section C.5.3.2**, External Hosted Operations, for detailed system administration needs in support of training.

h. Deliver training through any reasonable and available means including VTC, Defense Collaboration Services (DCS), and Mobile Training Teams (MTTs).
i. Develop, sustain, and update the PL's library of products to ensure all training is applicable to the current production environment.
j. Ensure quality production of Interactive Multimedia Instruction (IMI), IAW U.S. Army TRADOC Regulation 350-70-2 (http://www.tradoc.army.mil/tpubs/index.htm), for the specified courses and corresponding tasks.
k. Deliver and maintain user access to appropriate training.
l. Provide an innovative approach and cost avoidance to end-user training.
m. Provide end user training in both CONUS and OCONUS locations.

The chart below depicts the minimum number of classes in a twelve-month performance period.

Trips	Classes (Can run concurrently)	Locations (Government-Provided)	Curriculum
2	2-4	PEC	All applications
2	2-4	ARRTC	All applications
2	4	West Coast	All applications
2	4	East Coast	All applications

Note: Currently, class size averages 12-20 students per class.

C.5.7 TASK 7 – INNOVATION

PL RCAS-FMS PO has a history of providing improvement and innovation to customer and mission requirements as they arise in support of various technical initiatives within PL RCAS-FMS PO cognizance. The contractor shall be prepared to provide innovation in support of tasks 1 through 6. The Government will determine when innovation support is required IAW **Section H.19** – Technical Direction. The contractor shall analyze and review the latest advances in technology and best industry practices to optimize the current systems. The contractor shall develop a process to implement initiatives that are compliant with DoD/Army policy. The contractor shall define an incremental approach to achieving the required capability and perform the following:

a. Analysis (**Section F, Deliverable 67**)
    1. Assess the current baseline and identify opportunities for improvement.
    2. Establish baseline capacity and performance metrics for benchmarking purpose.
    3. Provide recommendation for implementing innovations.
    4. Identify any risks associated with the recommendations.
b. Design (**Section F, Deliverable 68**)
    1. Deliver a Detailed Design which shall specify:
        i. Concept of Operations (CONOPS) including at minimum cybersecurity and migration strategies.
        ii. Interface specification.
        iii. Detailed process flows.
        iv. Detailed configurations specifications.
        v. Applicable DoDAF views.

2. Deliver a Test Strategy considering:
    i. Integration testing.
    ii. Migration testing.
    iii. Regression testing.
    iv. Performance testing.
    v. Cybersecurity, DR, and business continuity capabilities.
3. Prototype/Proof of Concept.

c. Monitor and Report Innovation Results (**Section F, Deliverable 69**)
    1. Provide qualitative and quantitative results comparing the planned benefits identified in the Analysis to actual benefits achieved.

Once an innovation has been approved by the PL RCAS-FMS TPOC and FEDSIM COR, implementation of the innovation will be conducted under Tasks 1 through 6 or Task 8.

C.5.8 TASK 8 – SURGE/SPECIAL PROJECTS SUPPORT (OPTIONAL)

PL RCAS-FMS PO has a history of providing rapid responses to customer and mission requirements as they arise in support of various technical initiatives within PL RCAS-FMS PO cognizance. The contractor shall be prepared to provide surge/special projects in support of tasks 1 through 6. The Government will determine when surge/special support is required IAW **Section H.19** – Technical Direction.

At minimum, the contractor shall provide the following support under this task:

a. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
b. Travel as required to customer sites to install new software/hardware.
c. Identify omissions and errors in requirements and recommend optimum approaches.
d. Develop and test systems design for approved technical initiative projects.
e. Plan work schedules and perform customer support activities involving software design, development, testing, and program management.
f. Review documentation and provide documentation of errors/anomalies (redlines as applicable).
g. Provide comments to documentation at the guidance of the Government.